BY ORDER OF THE
SECRETARY OF THE AIR FORCE

AIR FORCE INSTRUCTION 33-204

1 OCTOBER 1997

AIR FORCE MATERIEL COMMAND
Supplement 1

5 January 1999

Communications and Information

INFORMATION PROTECTION SECURITY AWARENESS, TRAINING, AND EDUCATION (SATE) PROGRAM

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

NOTICE: This publication is available digitally on the SAF/AAD WWW site at: http://afpubs.hq.af.mil. If you lack access, contact your Publishing Distribution Office (PDO).

OPR: HQ AFCA/GCII (Dr T.J. Mucklow)
Supersedes AFI 33-204, 15 December 1994

Certified by: HQ USAF/SCXX (Lt Col Webb)
Pages: 11
Distribution: F

This instruction implements Air Force Policy Directive (AFPD) 33-2, *Information Protection,* and applicable parts of National Institute for Standards and Technology Special Publication 500-172, *Computer Security Training Guidelines;* National Telecommunications and Information Systems Security Directive Numbers 500 and 501; Executive Order 12958, *Classified National Security Information*; Office of Management and Budget (OMB) Circular A-130, *Management of Federal Information Resources*, Appendix 3, *Security of Federal Automated Information*; Office of Personnel Management, 5 CFR Part 930, Programs *for Specific Positions and Examinations*; and Title 40 U.S.C. , *The Computer Security Act of 1987*, 17 April 1995. It provides guidance and responsibility for establishing and managing the SATE Program; defines program goals; and applies to all military and civilian Air Force personnel. It also supports the awareness and education programs outlined in other publications such as Air Force Instruction (AFI) 33-203, *The Air Force Emission Security Program*. Additional security instructions and memoranda are listed in Air Force Indexes (AFIND) 2, *Numerical Index of Standard and Recurring Air Force Publications*; and 5, *Specialized Information Protection Publications*. Air Force Manual (AFMAN) 33-270, C4 Systems Security Glossary, explains other terms. Personnel may use extracts from this AFMAN. Direct questions or comments on the contents of this instruction through appropriate command channels to HQ AFCA/GCII, 203 W Losey Street, Room 2025, Scott AFB IL 62225-5234. Refer recommended changes and conflicts between this and other publications to HQ AFCA/XPXP, 203 W Losey Street, Room 1060, Scott AFB IL 62225-5233, using AF Form 847, **Recommendation for Change of Publications.** Major commands (MAJCOM), field operating agencies (FOA), and direct reporting units (DRU) send one copy of their supplement to HQ AFCA/XPXP. See attachment 1 for a list of references, abbreviations, and acronyms.

(AFMC) This supplement further defines responsibilities and procedures for establishing and managing the Security Awareness, Training, and Education (SATE) Program under AFMC jurisdiction. Air Force

has changed the designation of Information Protection (IP) to Information Assurance (IA). Each base IA office may develop a supplement outlining local procedures. Base supplements may add to but not take away from the AFI and major command supplement. This supplement supersedes all AFMC IA policy letters relating to this subject area dated prior to the publication of this supplement. It does not apply to the Air National Guard or US Air Force Reserve units and members.

SUMMARY OF REVISIONS

This revision changes all references from the term "C4 systems security" to read: "information protection." It requires personnel to administer awareness-level training by using computer based training, deletes reference to mission security briefings, and changes "HQ AFC4A/SYI" to "HQ AFCA/GCII." It also deletes the C4SSTAG as a working group. This revision also includes references to Information Operations (IO) and Information Warfare (IW).

AFI 33-204, 1 October 1997, is supplemented as follows:

Section A—General Information

1. Introduction . This instruction describes and defines the security awareness, training, and education (SATE) program goals, objectives, and standards. The SATE program is a single, integrated communications awareness, training, and education effort covering communications security (COMSEC), computer security (COMPUSEC), and emission security (EMSEC) disciplines. The program emphasizes information protection precepts and promotes consistent application of security principles in the use of Air Force information systems.

2. Goal . The goal of the SATE program is to make sure all personnel understand the necessity of, and practice of safeguarding information processed, stored, or transmitted on all information systems. Personnel must know how to protect these systems against sabotage, tampering, denial of service, espionage, fraud, misappropriation, misuse, or release to unauthorized persons by applying various information protection countermeasures. The SATE program objectives provide a basis for establishing the required learning objectives in all training methods.

3. Objectives . The objective of the SATE program is to train individuals to:

3.1. Understand the inherent weaknesses in information systems and the potential harm to national security due to the improper use of information systems.

3.2. Keep informed of the threats (including human intelligence) to, and vulnerabilities of, information systems.

3.3. Take necessary measures to protect information generated, stored, processed, transferred, or communicated by information systems.

3.3. (AFMC) Information requiring protection within AFMC is designated: classified information (secret and top secret) and sensitive information.

3.4. Recognize practices and conditions that create vulnerabilities in information systems, and use established security procedures to address them.

3.5. Recognize the potential damage to national security if COMSEC material is compromised and understand the security measures required to protect this material.

3.6. Protect information systems against denial of service and unauthorized (accidental or intentional) disclosure, modification, or destruction of information systems and data.

3.7. Understand how COMPUSEC, COMSEC, and EMSEC relate to the overall protection of information generated, processed, stored, or transferred by information systems.

Section B—Training

4. General Requirements . All military and civilian personnel will receive four types of SATE training: accession, initial/recurring, awareness, and specialized. An individual trained in information protection principles and concepts will conduct this training.

4.1. For COMSEC training policy guidelines, consult AFKAG-1, *Air Force Communications Security (COMSEC) Operations*, AFI 33-211, *Communications Security (COMSEC) User Requirements*, and *AFI 33-209 Operational Instruction for Secure Telephone Unit (STU-III), Type 1.*

4.2. For EMSEC training policy guidance, see AFI 33-203, *The Air Force Emission Security Program.*

4.3. For COMPUSEC training guidelines, see AFSSM 6000, *Information Protection Training Guide.*

5. Accession Training .

5.1. Headquarters Air Education and Training Command (HQ AETC) will:

5.1.1. Conduct information protection accession training during initial military training (basic military training, Officer Training School, Air Force Reserve Officer Training Corps, and specialized training in Air Force specialty code [AFSC] awarding courses).

5.1.2. Train students on basic information operations (IO) and information warfare (IW) concepts to establish a foundation of information protection awareness.

5.1.2.1. Make sure they understand that certain vulnerabilities and threats exist in information systems and require protection.

5.1.3. Define information protection by including the concepts of COMSEC, COMPUSEC and EMSEC.

5.1.4. Stress that there is a point of contact for SATE at every Air Force unit and at the wing information protection Office.

5.1.5. Administer information protection training, through Air University, to students attending Senior Noncommissioned Officer Academy, Squadron Officer School, Air Command and Staff College, and Air War College.

5.1.6. Coordinate information protection training material with HQ AFCA/SYSI through the MAJCOM SATE manager.

5.2. The Air Force Personnel Center will provide information protection training for Palace Acquire accessioned civilians through the civilian career programs.

6. Initial/Recurring Training Requirements . The SATE program managers customize this training to accomplish the SATE program objectives prescribed in paragraph 3. Convey the degree of reliance on information systems, the potential consequences arising from the lack of secure information systems, the organization's commitment to secure information systems, and the means by which users can protect information systems. Mission sensitivity and the potential for mission degradation from the lack of proper information protection must influence the design of recurring and awareness training. This includes interruption or exploitation of service, exploitation through interception, unauthorized electronic access or related technical threats, and corruption through falsification of information or damages to storage media. Use computer based training for both initial and recurring information protection training. Currently, you must use AF SAFEWARE to meet the training requirements.

6.1. Initial/Recurring Training of at least one hour annually:

6.1.1. Air Force military, civilian, and contract personnel will receive information protection awareness-level training within 60 days of permanent change of station/permanent change of assignment to a new organization.

6.1.1.1. Personnel will take appropriate computer based training (CBT) modules before they are issued user IDs or passwords or otherwise granted network access.

6.1.1.2. Personnel will take appropriate CBT module(s) before they are issued a crypto ignition key (CIK) for any secure voice telephone.

6.1.2. Personnel who do not use an information system in the performance of duties are exempt from the use of CBT tools in initial, recurring, or specialized information protection awareness-level training.

6.1.2.1. MAJCOM/wing managers will ensure that selected CBT modules meet organizational mission requirements. MAJCOMs and wings will add modules for meeting mission-unique training requirements.

6.1.2.1. (AFMC) Includes contractor personnel when providing IA training to all system users.

6.1.3. Use command-tailored, HQ AFCA-produced, or other educational materials to reemphasize information protection obligations.

6.2. (Added-AFMC) Local OSI will provide Human Intelligence (HUMINT) information.

7. Awareness Training . The SATE program managers satisfy awareness training requirements by displaying information protection-related awareness aids, using public service announcements, or providing applicable articles from unit, base, and command publications to unit personnel. Managers will encourage the use of information protection screen savers and take advantage of local cable public service channels (Armed Forces Radio and Television Service overseas) to advance information protection awareness.

8. Specialized Training (Formal Course Integration). HQ AETC and the United States Air Force Academy (USAFA) will provide students with an understanding of IO and IW and of the threat to, and vulnerabilities of Air Force information systems, a knowledge of countermeasures available to overcome the threat, and ways to apply the countermeasures.

8.1. This instruction provides general guidance for integrating information protection education and training into the Air Force accession programs, AFSC-awarding courses, formal schools, and professional military education courses.

8.2. Base the depth of other formal training programs coverage on the students' potential to become involved in planning, programming, managing, operating, or maintaining information systems, or who work routinely with such material. The courses will emphasize the threat to and vulnerabilities of information systems, the information protection countermeasures available to overcome the threat, and ways to apply those countermeasures.

8.3. USAFA and HQ AETC courses will also address those aspects of information protection that could affect the success of tactical and strategic operations.

8.4. All course developers, normally Air Force specialty functional managers, will coordinate information protection training material with HQ AFCA/GCII through the MAJCOM functional and SATE managers. HQ AFCA/GCII will provide advisory assistance for program development. HQ AFCIC/XPF is the Air Force specialty functional manager for AFSC 3CXXX, Communications-Computer Systems, and 33SX, Communications-Information Systems.

9. Report Control Symbol: HAF-SC (A) 9604, Information Protection Security Awareness, Training, and Education Utilization Report. This annual report provides a basis for assessing the impact of information protection training on mission accomplishment. SATE is part of the overall Information Protection Program outlined in AFPD 33-2.

9.1. MAJCOM SATE Program Managers:

9.1.1. Metrics reporting is designated "emergency status code Command and Control." Continue reporting during emergency conditions, normal precedence. Submit data requirements as prescribed, or as soon as possible after submission of priority reports.

9.1.2. Continue reporting during MINIMIZE.

9.1.3. Establish specific command procedures to acquire, compile, and report command information (see Table 1).

9.2. The wing SATE program manager consolidates figures from unit SATE managers for initial and refresher training and forwards this information to the appropriate MAJCOM. The MAJCOM will consolidate their wing reports. Submit consolidated MAJCOM/FOA/DRU SATE Metrics Reports to HQ AFCA/GCII no later than 15 January for each preceding calendar year. **NOTE**: Table 1 outlines the format.

Table 1. SATE Utilization Report Format.

Month	Initial	Recurring
January	1,311	10,111
February	5	4,502
February	5	4,502
March	16	916
April	99	412
May	921	8
June	73	1,110
July	88	124
August	89	412
September	9	502
October	1	174
November	90	392
December	2	26
Totals	2,704	18,689
Total Personnel Trained: 21,393		
Total Personnel Assigned to the Command: 23,999		
Percentage Trained: 89 Percent		

Section C—Roles and Responsibilities

10. Headquarters United States Air Force . The Director, Communications and Information (HQ USAF/SC) is the Air Staff office of primary responsibility for the Air Force Information Protection Security Awareness, Training, and Education Program. HQ USAF/SC delegates information protection, including information protection SATE responsibilities, to HQ AFCIC/SYNI.

11. Headquarters Air Force Communications Agency/Information Protection Division (HQ AFCA/GCI):

11.1. Manages the SATE program.

11.2. Guides, monitors, and assists MAJCOM program managers as they implement their SATE program efforts.

11.3. Performs staff assistance visits to requesting MAJCOMs.

11.4. Develops generalized educational material, such as pamphlets, videotapes, and awareness aids, to support the overall Air Force information protection missions.

11.5. Prepares specialized briefings and assists MAJCOMs as requested.

11.6. Reviews and approves developed SATE program materials, including implementing documents submitted by Air Force personnel.

11.7. Establishes a SATE information crossfeed program.

11.8. Develops and publishes information protection articles and/or other works.

11.9. Is the office of primary responsibility for CBT/awareness, training, and education software.

11.10. Administers the Air Force Information Protection World Wide Web Home Page to disseminate information protection awareness, information, and crossfeed.

12. Major Commands :

12.1. Participate in the Air Force SATE program and support their wing and tenant SATE program managers.

12.2. Designate a primary and an alternate individual to implement and manage the command SATE program. Provide HQ AFCA/GCII with the names, grades, office symbols, e-mail, facsimile and telephone numbers of these individuals.

12.2. (AFMC) The commander or director of the organization managing the local IA office will provide the AFMC IA office (AFMC CSO/SCSN) with the names, grades, office symbols, telephone numbers and Email addresses of these individuals when assigned, and as changes occur. The AFMC IA office will approve or disapprove waivers.

12.3. Work with HQ AFCA/GCII to develop command-oriented information protection educational materials, such as pamphlets, news articles, awareness aids, and videotapes to support the command SATE program, as needed. Provide all materials to subordinate units for use and to HQ AFCA/GCII for review and crossfeed.

12.4. Develop and publish command-oriented information protection articles in command news media.

12.5. Conduct workshops for wing SATE program managers at least biennially.

12.6. Provide SATE program materials and guidance to Air Force Reserve and Air National Guard units gained upon mobilization in coordination with Headquarters Air Force Reserve and National Guard Bureau OPRs.

12.7. Provide information protection guidance and assistance, as needed, to operations security (OPSEC) program managers through the command OPSEC manager.

12.7. (AFMC) The command OPSEC manager is HQ AFMC/SF.

12.8. Include information protection educational materials in command-developed courses as outlined in paragraph 12.3.

12.9. Make sure government contractors follow the provisions of this instruction when using information systems in support of Air Force contracts to generate, process, store, transfer, or communicate information, as applicable.

12.9. (AFMC) The local Chief of Security Forces (SF) or Chief of Acquisition Security (AS) has cognizance over contractors requiring access to classified information on their installations as inter-

mittent visitors, visitor groups, or cleared facilities. Coordinate IA SATE requirements with the local SF or AS offices in an effort to benefit the customer by reducing the number of training seminars.

12.10. Perform staff assistance visits to requesting wings.

12.11. (Added-AFMC) A SATE program review will be conducted at AFMC bases, to include major program offices to ensure a sound SATE program is in effect. This review falls under the Information Protection Assessment and Assistance Program (IPAP), AFI 33-230. The compliance-oriented assessment will be scheduled at two-year intervals in conjunction with assessment of all IA disciplines, to include COMPUSEC, COMSEC, EMSEC, and SATE. A representative number of the base facilities will be visited to identify problem areas and laudable practices.

13. Air Force Field Operating Agencies and Direct Reporting Units:

13.1. May either maintain their own SATE programs, or participate in their supporting host wing's SATE program via a memorandum of agreement with the host.

13.2. Will follow policy in paragraphs 9, 12, and 15 of this instruction, should they elect to manage their own SATE programs.

13.3. Will follow policy guidance in paragraphs 16 and 17 of this instruction when participating in the supporting host-wing program.

13.4. Will submit copies of their memoranda of agreement with the supporting host-wing to HQ AFCA/GCII.

14. Wings. Make sure the host SC (or senior communications officer or commander) designates primary and alternate individuals to manage the wing SATE program. Make sure the primary SATE manager is knowledgeable about information system operations and forwards letters of appointment to the MAJCOM information protection office.

15. Wing Security Awareness, Training, and Education Program Managers:

15.1. Implement, manage, and conduct base-wide SATE programs using information protection educational materials provided by the host MAJCOM and HQ AFCA.

15.2. Provide information protection training to all information systems users, including all tenants, geographically separated/isolated field offices, detachments, and remote operating locations.

15.3. Make sure personnel make maximum use of information protection CBT packages, etc; posters; screen savers; educational videotapes; awareness aids; and briefings, and emphasize use of these training tools.

15.4. Place reminders of the need for positive information protection practices in base bulletins and other media to increase and reinforce information protection awareness.

15.5. Provide information protection awareness training for all wing and tenant unit SATE program managers, and crossfeed locally developed material between those unit managers and wing headquarters. The host wing will provide training when there is more than one wing assigned to the base.

15.6. Perform annual SATE staff assistance visits to host and tenant units.

15.7. Implement and serve as the wing point of contact for information protection CBT, which is a mandatory information protection ancillary training program. (See AFCAT 36-222*USAF Formal Schools*).

15.8. Provide awareness training to newly appointed host and tenant unit information protection program managers. Training should include what information protection CBT is and how to use it.

15.8. (AFMC) Ensure host tenant agreements which address the IA SATE program are maintained in the official SATE program records. Ensure tenant organizations participating in the base SATE program appoint a unit SATE manager.

15.9. Conduct biennial or more frequent SATE workshops for unit managers.

15.9. (AFMC) Maintain workshop minutes in the official IA SATE program records for a minimum of two years.

15.10. Provide information protection CBT reporting metrics to MAJCOM/FOA/DRU SATE managers as outlined in paragraph 9.

15.10. (AFMC) Report the annual RCS:HAF-SC(A) 9604, IA Security Awareness, Training, and Education Utilization Report in accordance with AFI 33-204, paragraph 9 and AFPD 33-2, Information Protection, to the AFMC IA office no later than 10 Jan each year, or as otherwise directed.

16. Unit Commanders. Appoint a unit SATE program manager and an alternate to administer the SATE program within their unit, normally as an additional duty. Provide a copy of the appointment memos to the wing SATE manager.

16. (AFMC) Base/Wing IA offices must provide the AFMC IA office with the name, grade, office symbol, e-mail address, and telephone number of appointed individuals in writing. Each IA office should have a primary and alternate SATE manager.

17. The Unit Security Awareness, Training, and Education Program Manager:

17.1. Ensures all newly assigned personnel receive information protection awareness training before they are issued user IDs and passwords, or granted network access, or within 60 days of arrival.

17.2. Coordinates this training with the wing SATE program manager as needed.

17.3. Administers the annual recurring information protection training for all required personnel including those from field offices, detachments, and operating locations in the local area that receive unit administrative support, through use of information protection CBT.

17.4. Circulates quarterly information protection articles and displays current awareness aids throughout the organization.

17.5. Supports and implements the wing SATE program.

WILLIAM J. DONAHUE, Lt General, USAF
Director, Communications and Information

Attachment 1

GLOSSARY OF REFERENCES, ABBREVIATIONS, ACRONYMS, AND TERMS

References

Executive Order 12958, *Classified National Security Information*

National Institute for Standards and Technology Special Publication 500-172, *Computer Security Training Guidelines*

National Telecommunications and Information Systems Security Directive Numbers 500, *Information Systems Security (INFOSEC) Education, Training, and Awareness* and 501, *National Training Program for Information Systems Security (INFOSEC) Professionals*

Office of Personnel Management 5 CFR Part 930, *Security of Federal Automated Information Resources*

Title 40 U.S.C. Section 759, *The Computer Security Act of 1987, 17 April 1995*

OMB Circular A-130, *Management of Federal Information Resources*, Appendix 3, *Security of Federal Automated Information*

AFCAT 36-2223, *USAF Formal Schools*

AFI 33-203, *The Air Force Emission Security Program*

AFIND 2, Numerical Index of Standard and Recurring Air Force Publications

AFIND 5, *Specialized Information Protection Publications*

AFKAG-1, *Air Force Communications Security (COMSEC) Operations*

AFMAN 33-270, *C4 Systems Security Glossary*

AFPD 33-2, *Information Protection*

Abbreviations and Acronyms

AETC—Air Education and Training Command

AFCA—Air Force Communications Agency

AFCAT—Air Force Catalog

AFDIR—Air Force Directory

AFI—Air Force Instruction

AFIND—Air Force Index

AFPC—Air Force Personnel Center

AFPD—Air Force Policy Directive

AFSC—Air Force Specialty Code

CBT—Computer Based Training

COMPUSEC—Computer Security

COMSEC—Communications Security

DRU—Direct Reporting Unit

EMSEC—Emission Security

FOA—Field Operating Agency

IO—Information Operations

IW—Information Warfare

MAJCOM—Major Command

OPSEC—Operations Security

SATE—Security Awareness, Training, and Education

USAFA—United States Air Force Academy

Terms

Communications Security (COMSEC)—Measures and controls taken to deny unauthorized persons information derived from telecommunications and to ensure the authenticity of such communications.

Computer Security (COMPUSEC)—Measures and controls that ensure the confidentiality, integrity, or availability of information systems assets including hardware, software, firmware, and information being processed, stored, and communicated.

Emission Security (EMSEC)—Protection resulting from all measures taken to deny unauthorized persons information of value that might be derived from intercept and analysis of compromising emanations from crypto-equipment, information systems, and telecommunications systems.

Information Operations (IO)—Those actions taken to affect adversary information and information systems while defending one's own information and information systems. IO is conducted throughout all phases of an operation, across the full spectrum of military operations, at every level of warfare. Information Operations require the integration of activities composed of gaining information (surveillance, reconnaissance and traditional intelligence collection), information exploitation (intelligence analysis and production; weather; navigation and positioning; and communications and information), and offensive and defensive capabilities.

Information Protection—Measures to protect friendly information systems by preserving the availability, integrity, and confidentiality of the systems and the information contained within the systems.

Information Systems—Any telecommunications and/or computer related equipment or interconnected system or subsystem of equipment that information systems used in the acquisition, storage, manipulation, management, movement, control, display, switching interchange, transmission, or reception, of voice and/or data, and includes software, firmware, and hardware. **Note:** This includes automated information systems.

Information Warfare (IW)—Information operations conducted during time of crisis or conflict to achieve or promote specific objectives over a specific adversary or adversaries.